

1 / 28

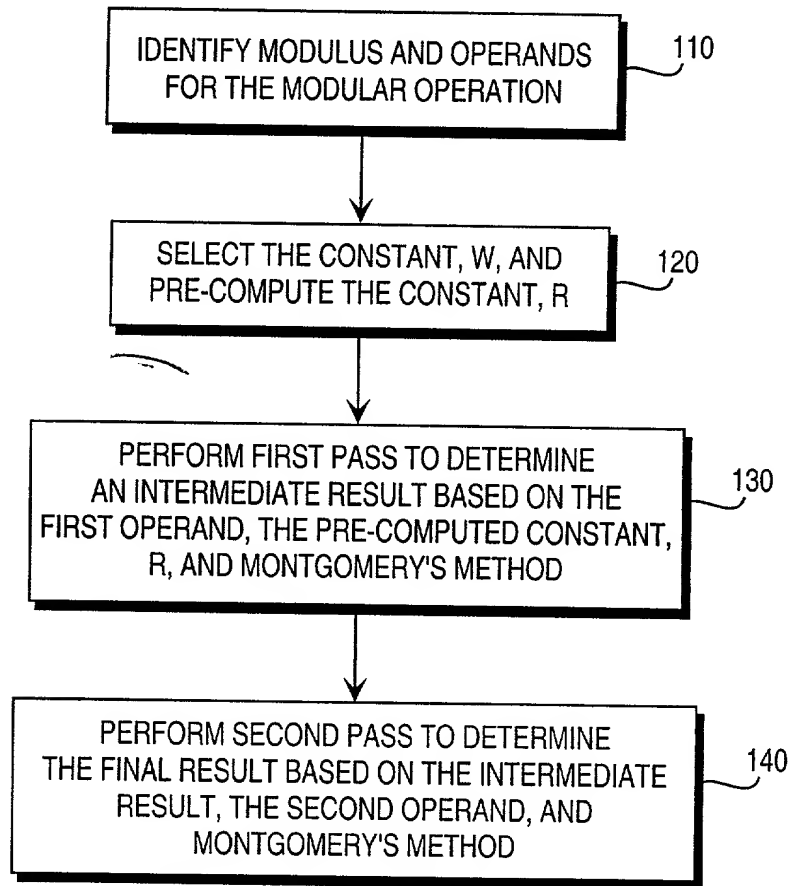


FIG. 1

2 / 28

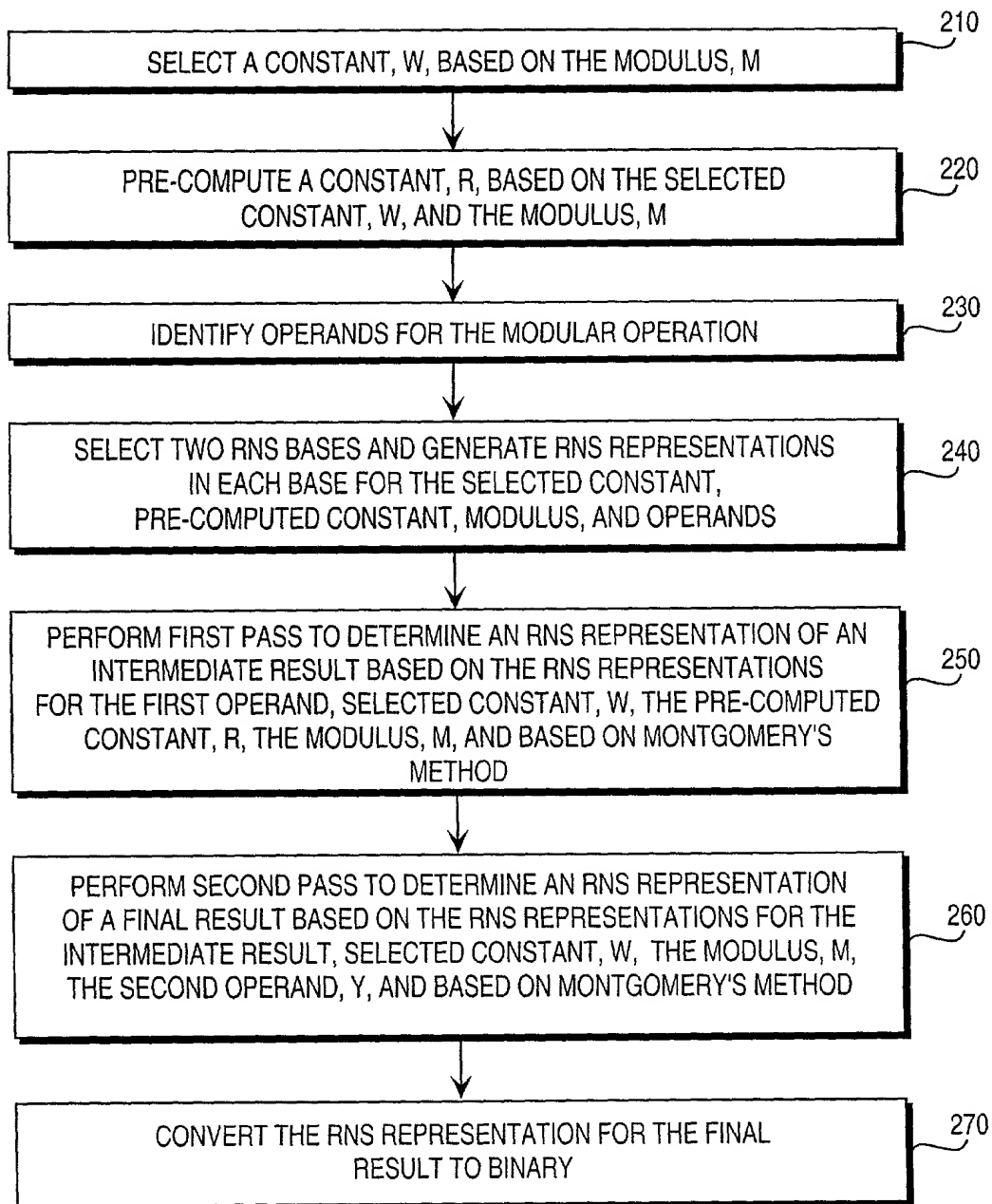


FIG. 2

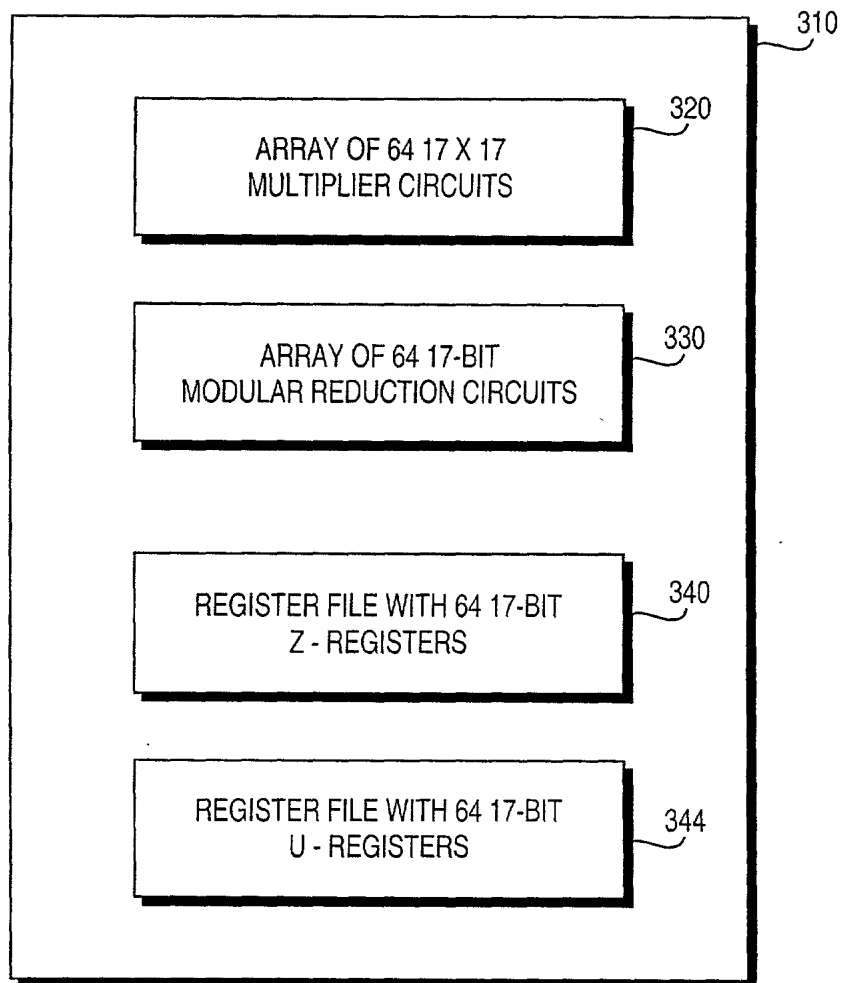


FIG. 3A

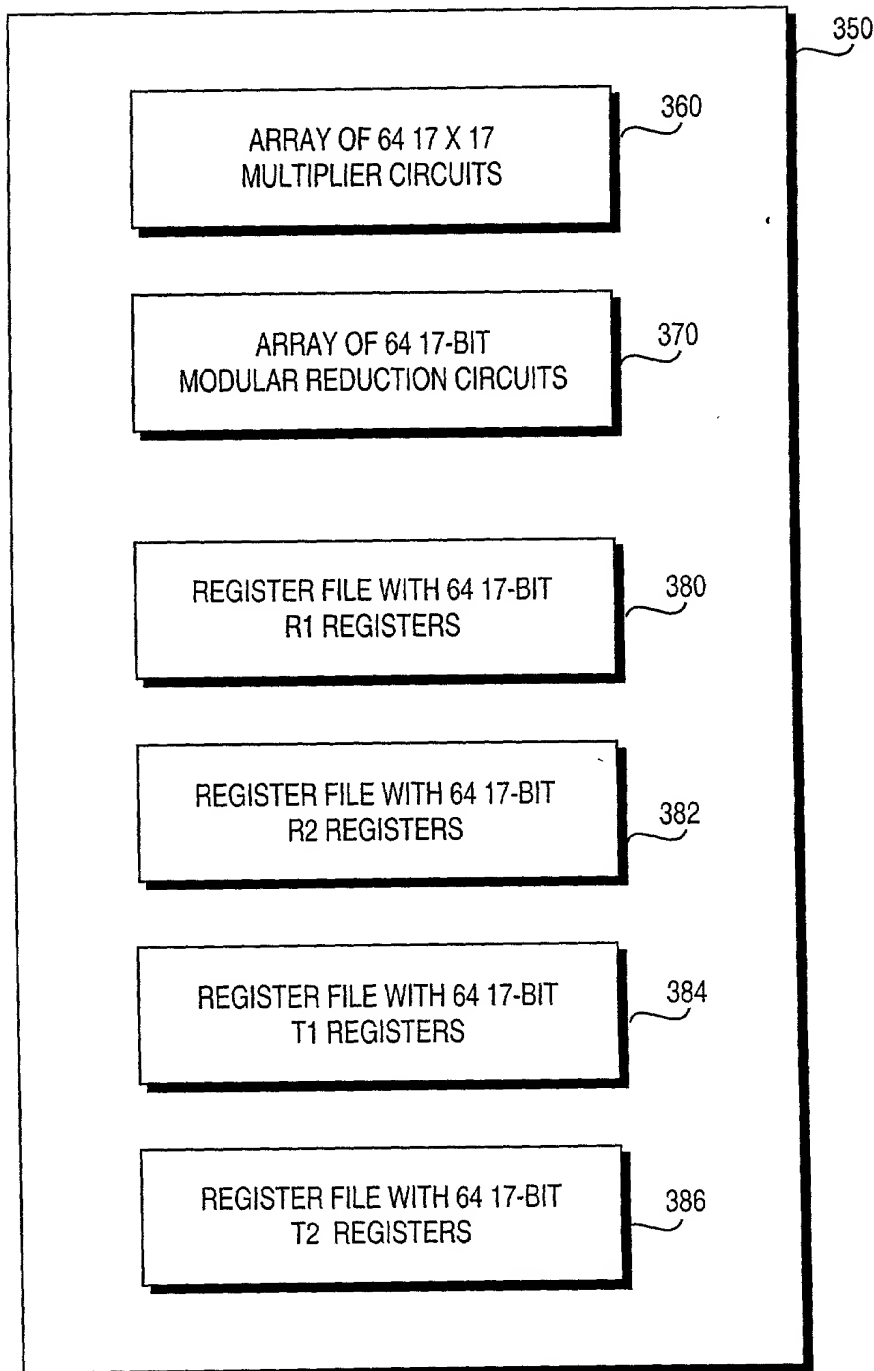


FIG. 3B

5 / 28

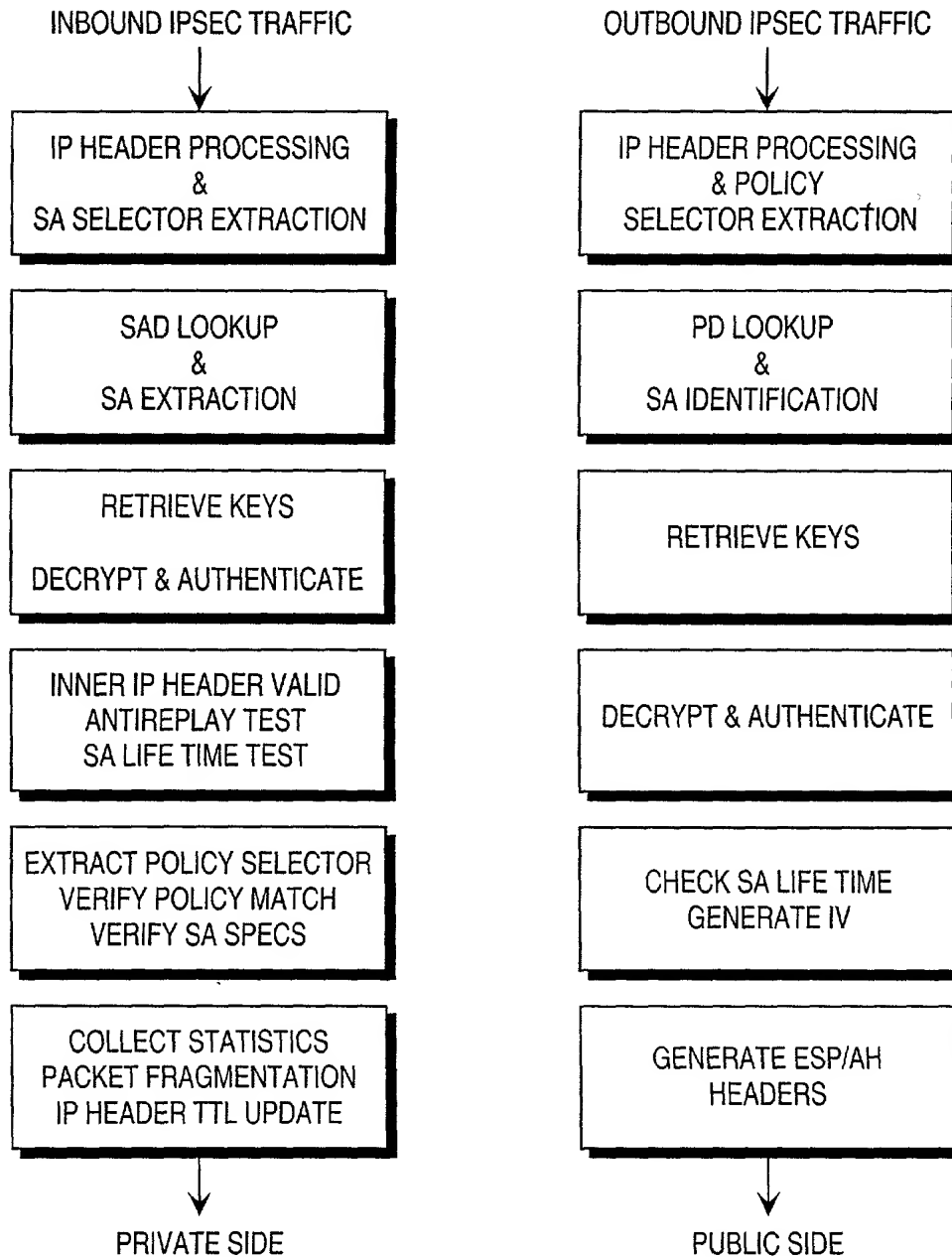


FIG. 4

6 / 28

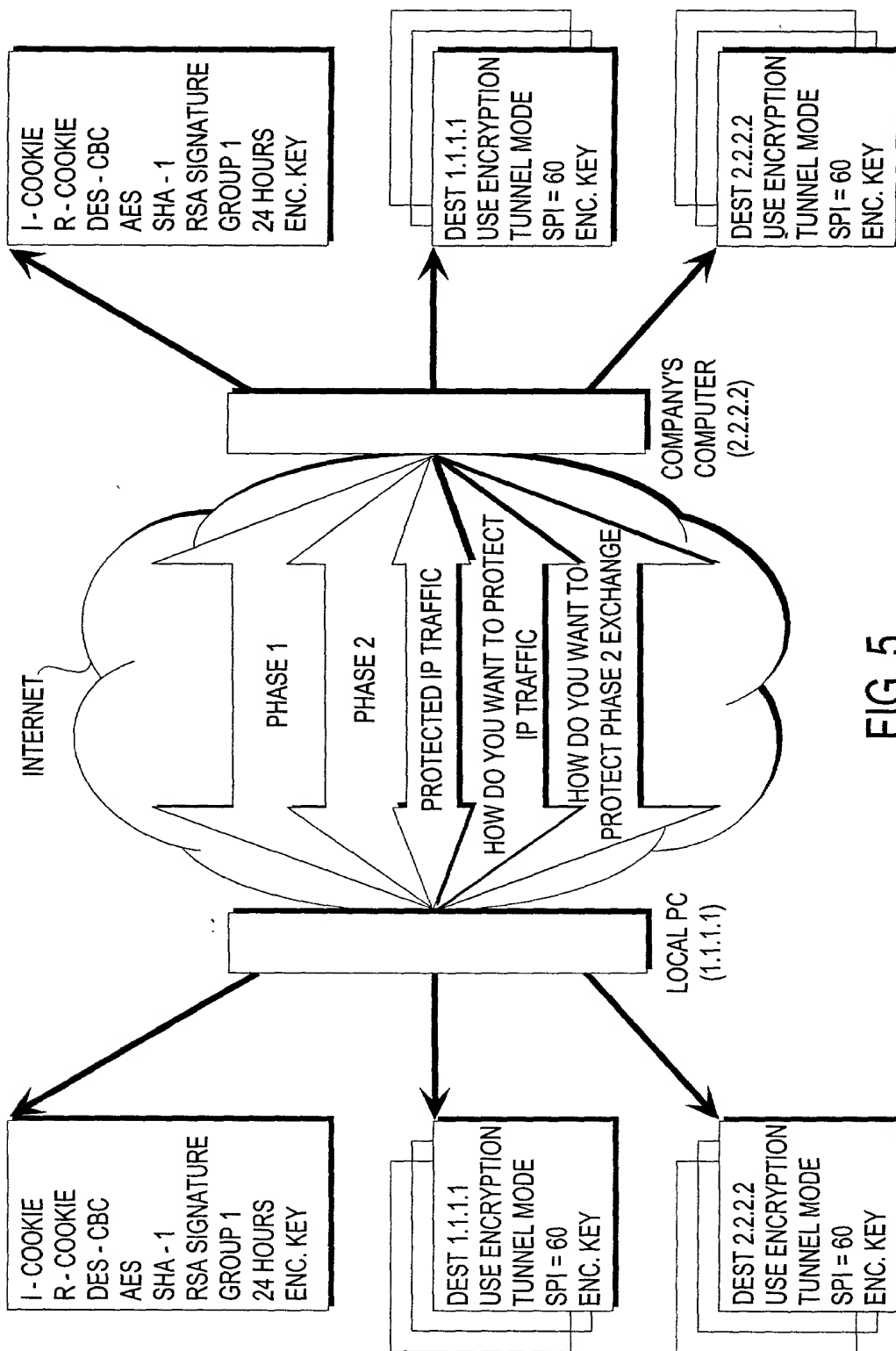


FIG. 5

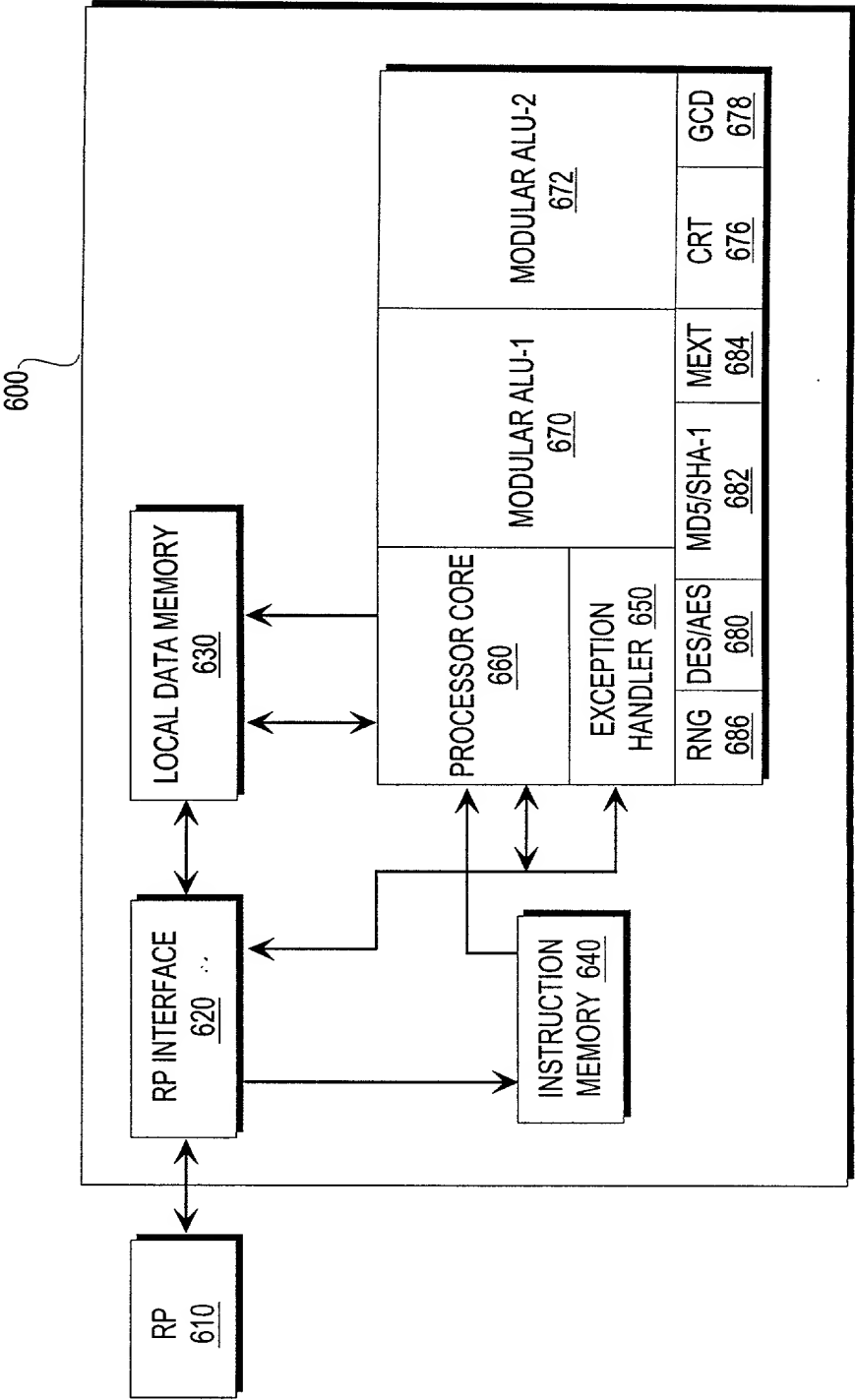


FIG. 6

8 / 28

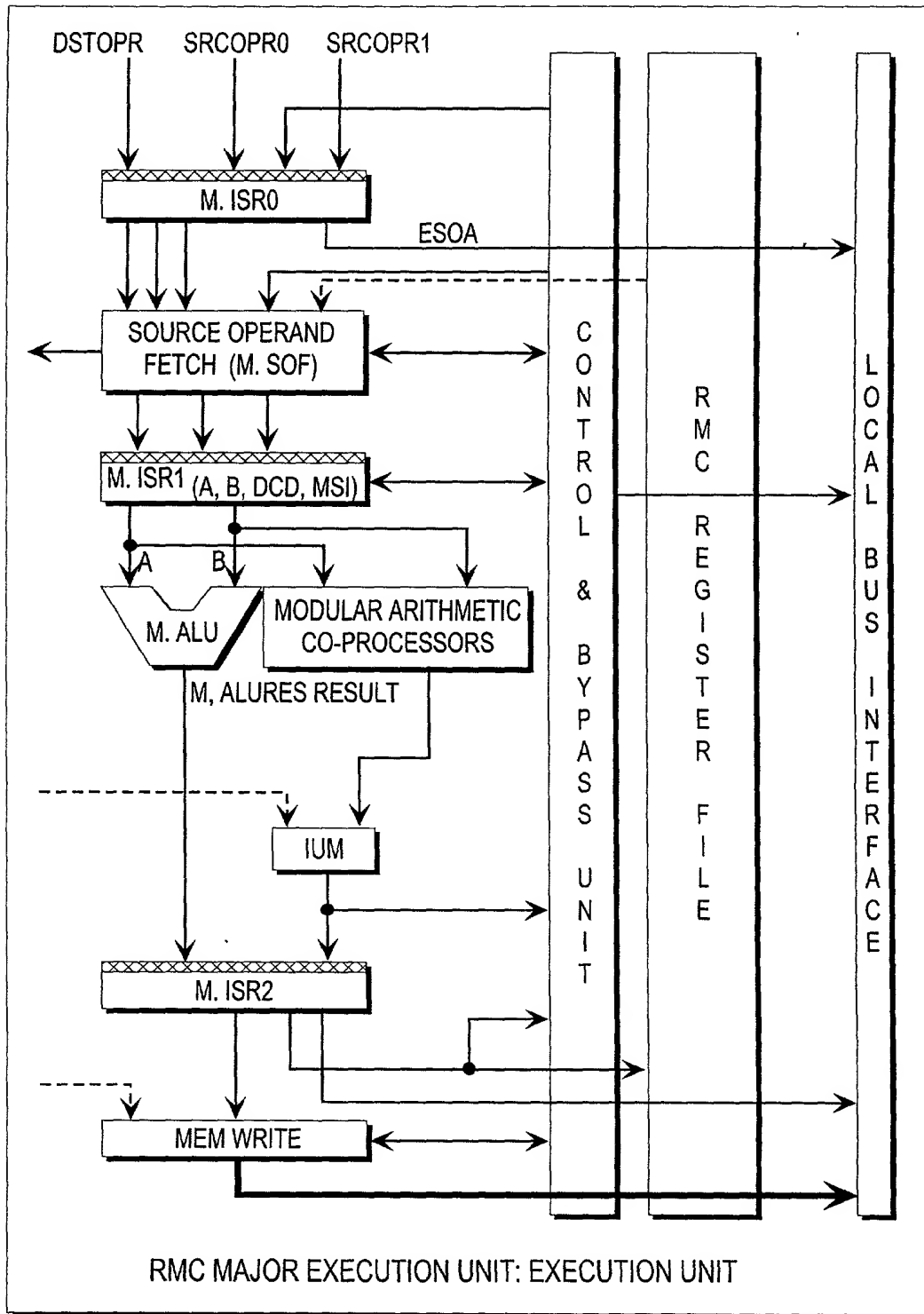


FIG. 7

9/28

NOTE: RECTANGULAR BLOCKS ON THE SAME HORIZONTAL LEVEL
OVERLAP EXECUTION TIMES.

\Leftarrow - SOURCE OVERWRITES DESTINATION REGISTER
 \otimes - MODULAR MULTIPLICATION WITH RESPECT TO W.
 \odot - MODULAR MULTIPLICATION WITH RESPECT TO V.
 \angle - RNS CONVERSION

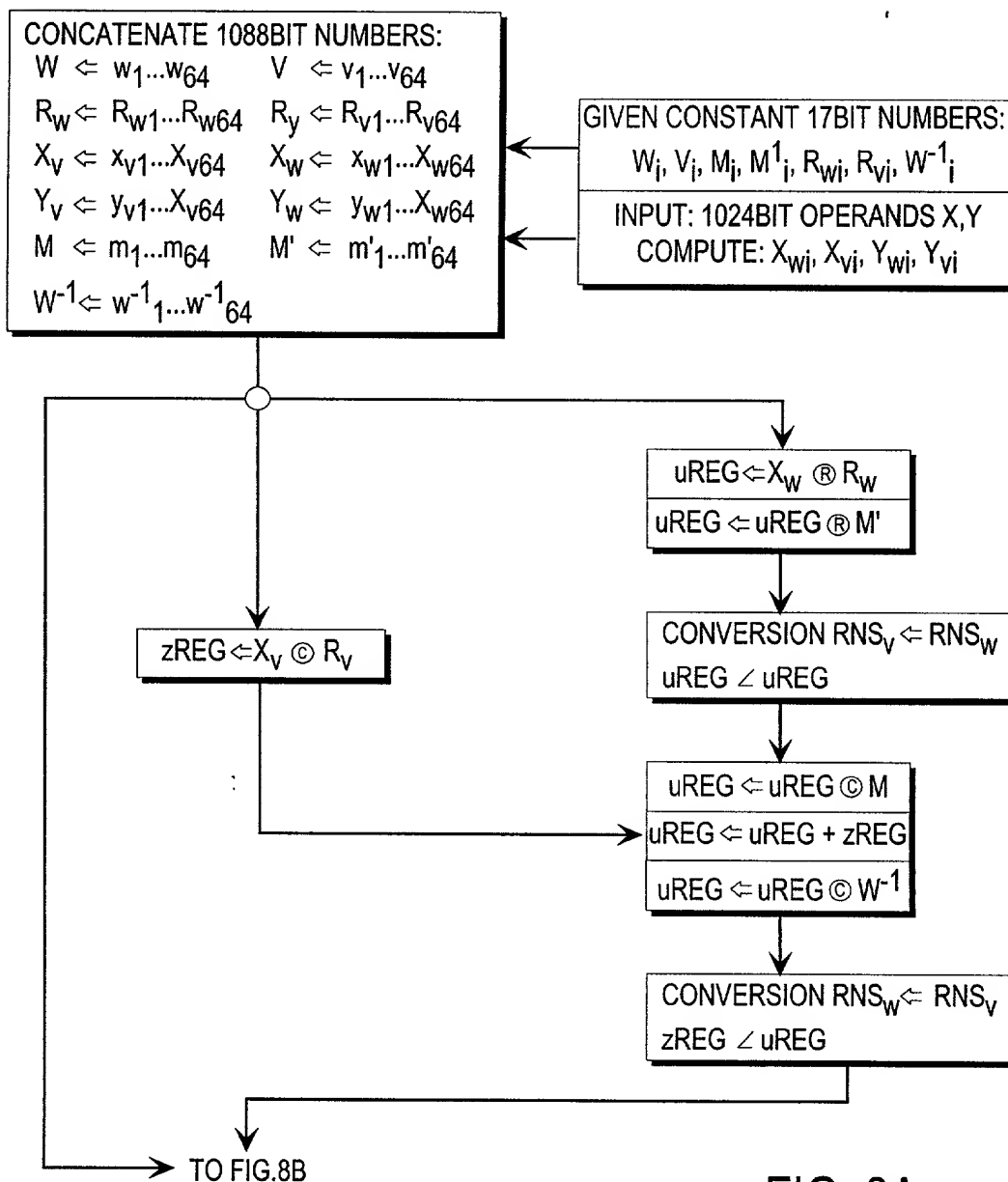


FIG. 8A

10 / 28

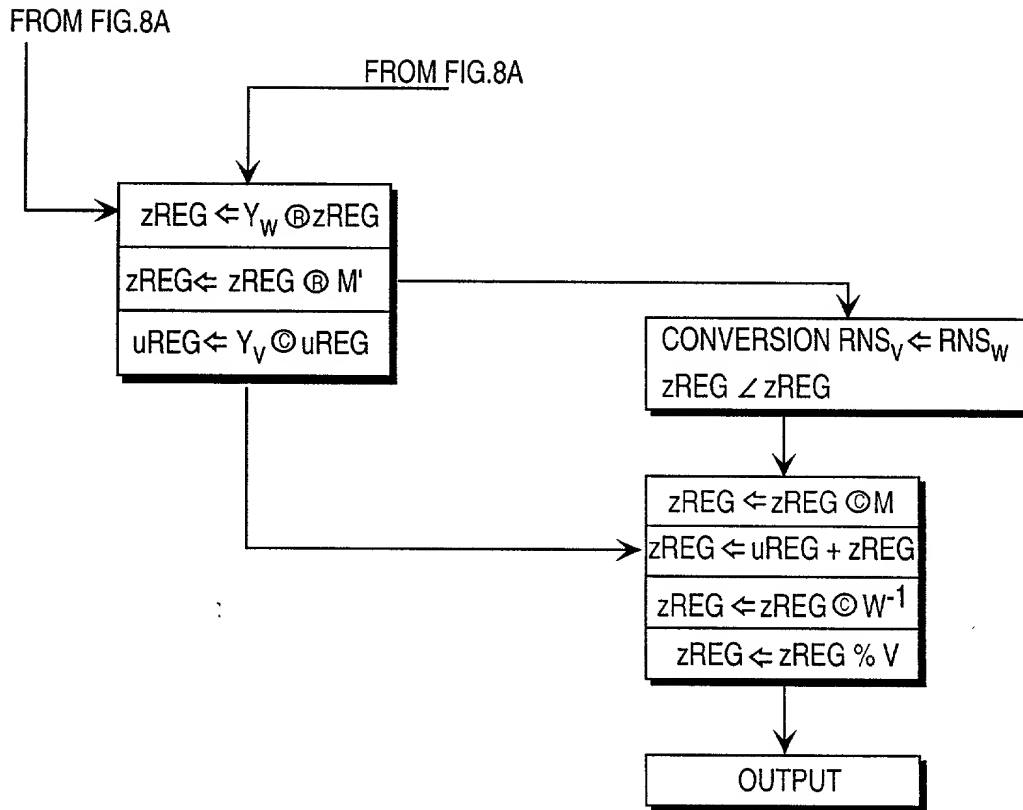


FIG. 8B

NOTE: ALL BUSSES ARE $64 \times 17 = 1088$ BITS WIDE.



12/28

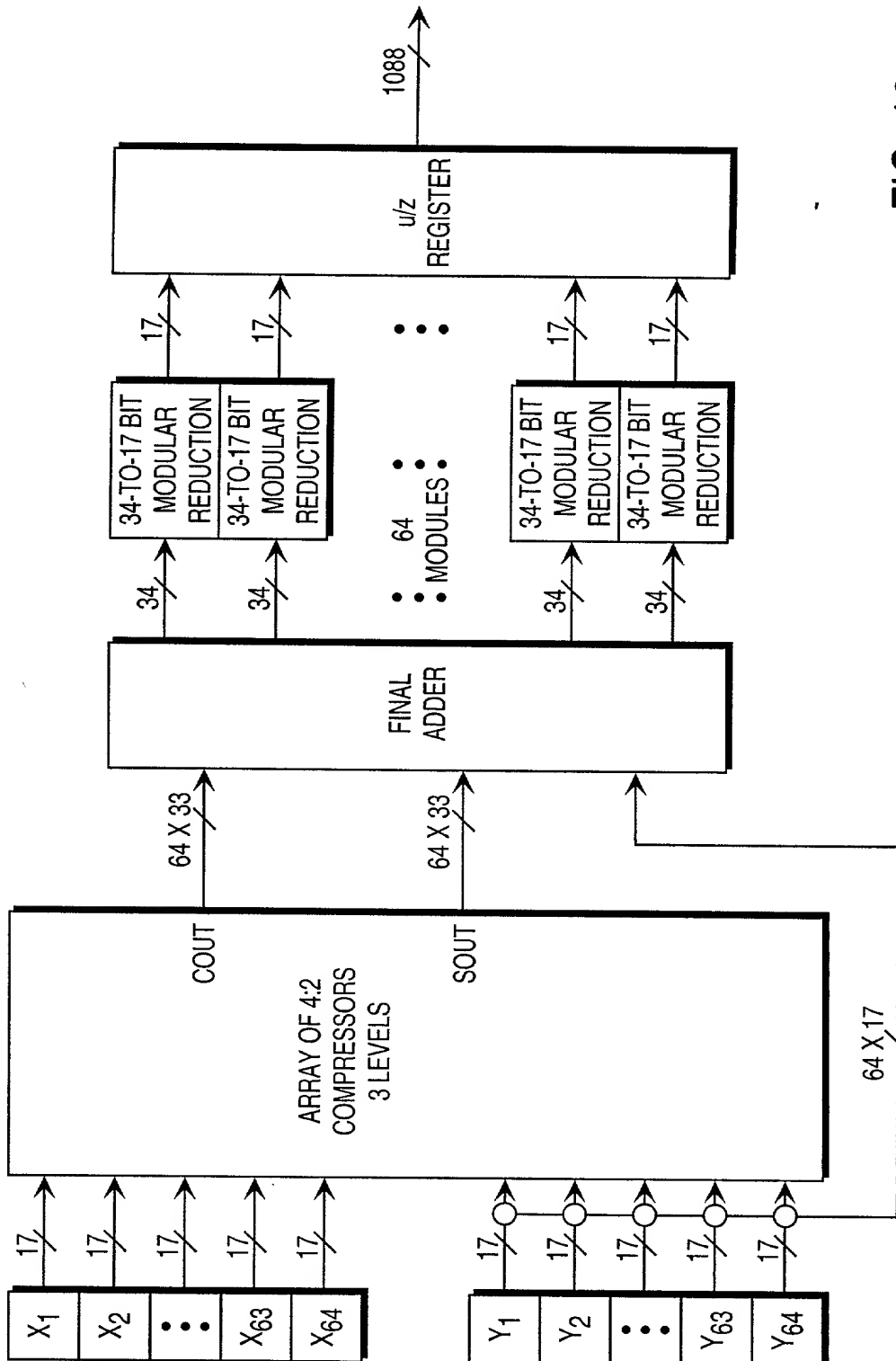


FIG. 10

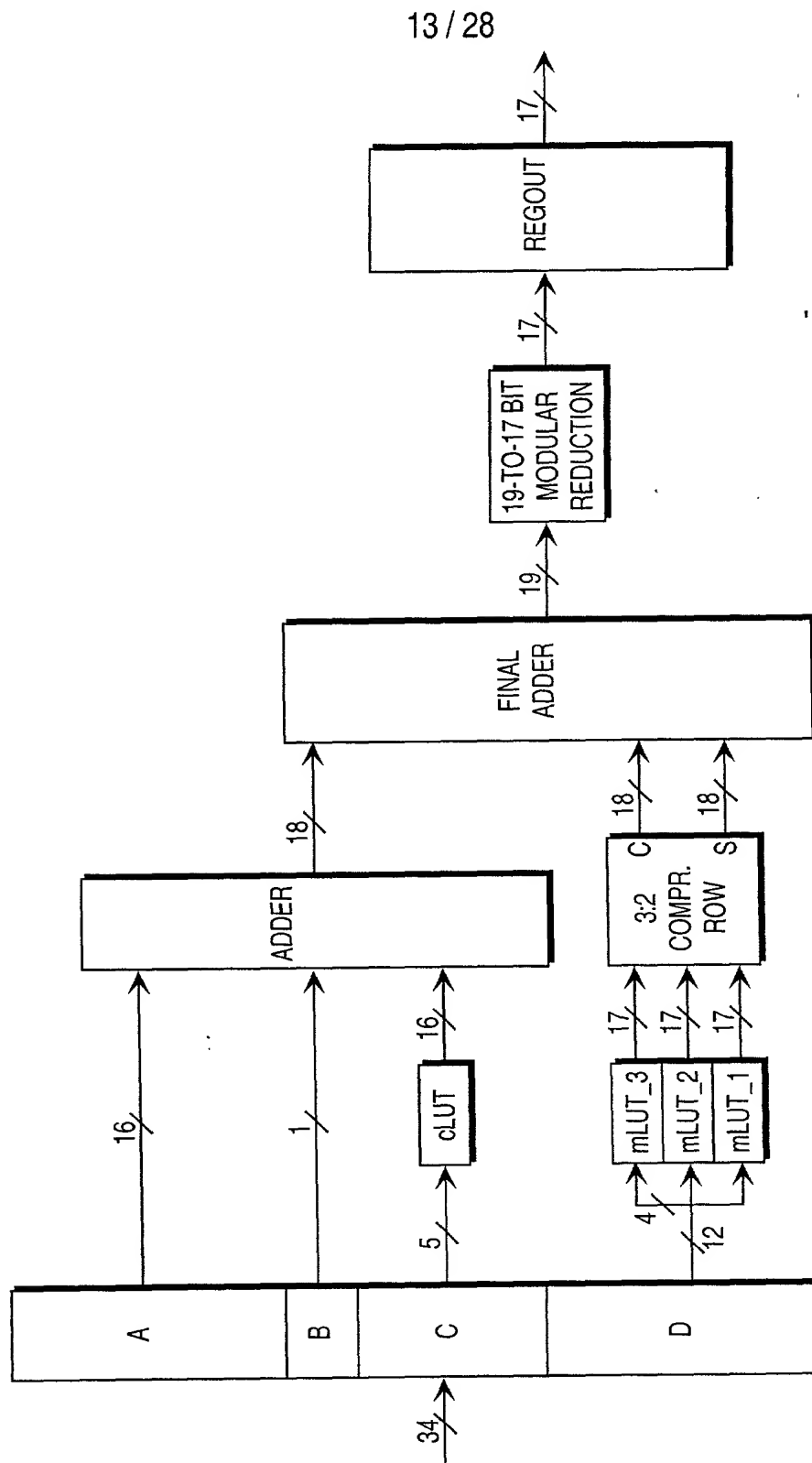


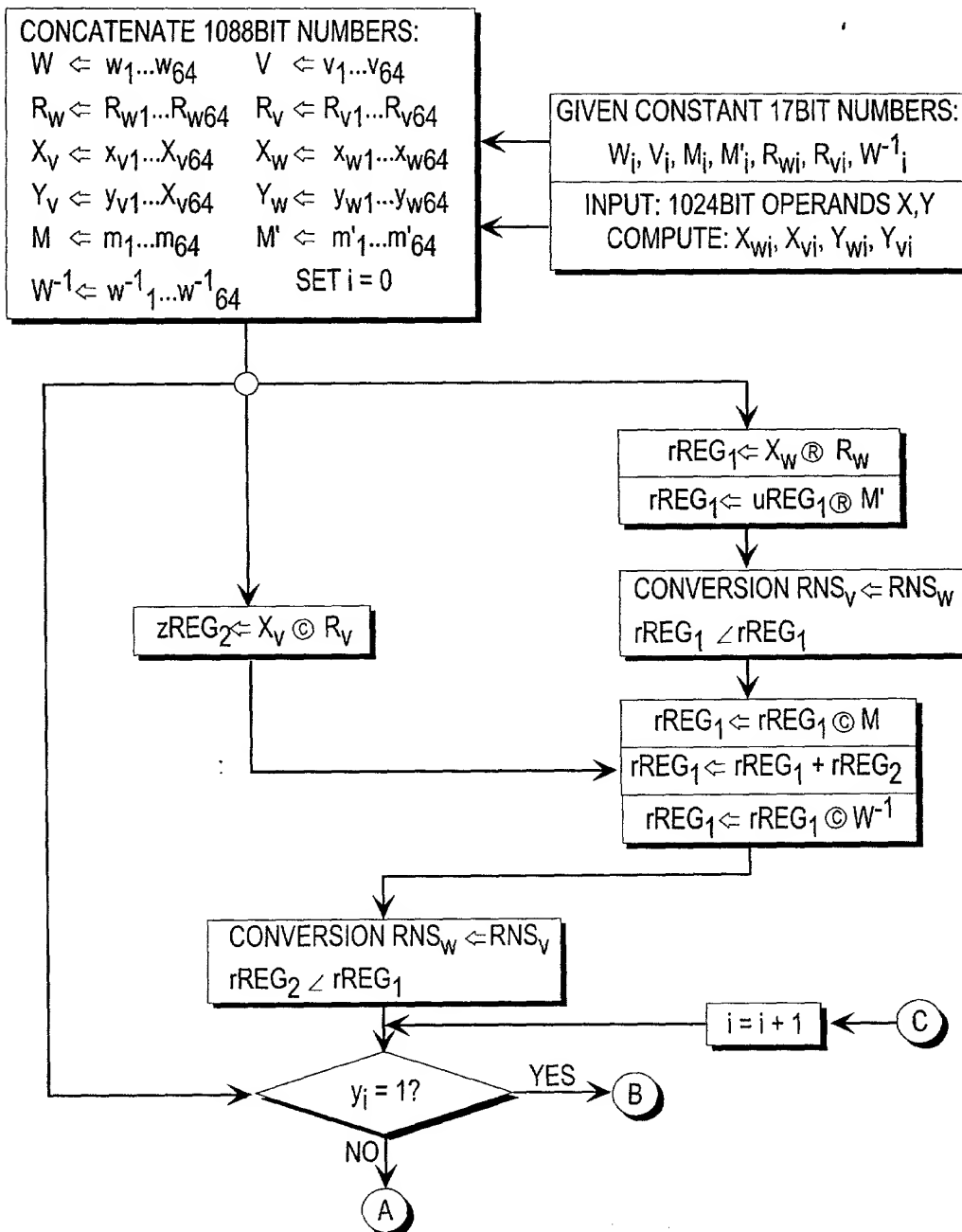
FIG. 11

14 / 28

NOTE: RECTANGULAR BLOCKS ON THE SAME
 HORIZONTAL LEVEL OVERLAP EXECUTION TIMES.

FIG. 12A

- ←- SOURCE OVERWRITES DESTINATION REGISTER
 ®- MODULAR MULTIPLICATION WITH RESPECT TO W.
 ©- MODULAR MULTIPLICATION WITH RESPECT TO V.
 ∠- RNS CONVERSION



15 / 28

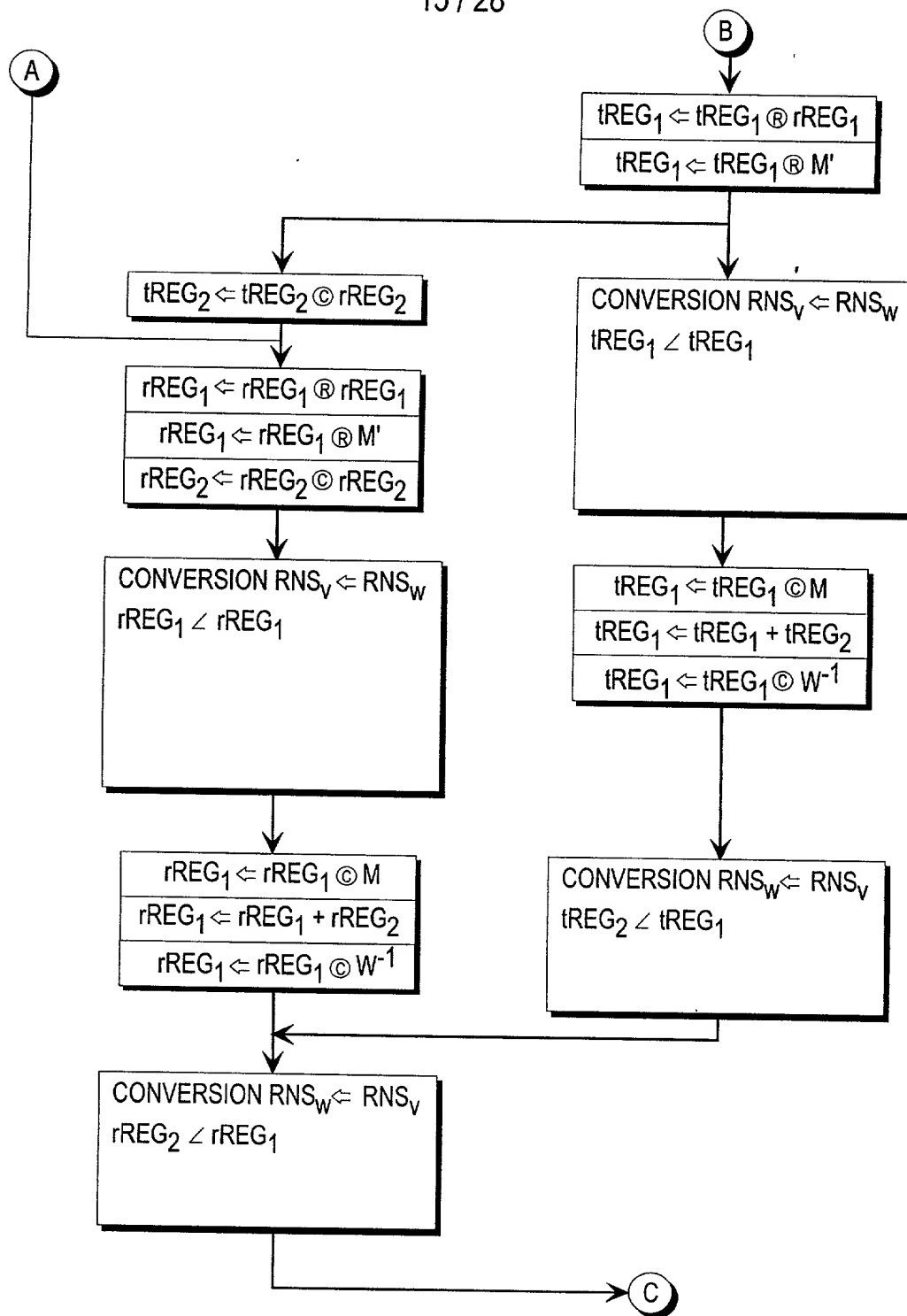


FIG. 12B

16 / 28

NOTE: ALL BUSSES ARE $64 \times 17 = 1088$ BITS WIDE.

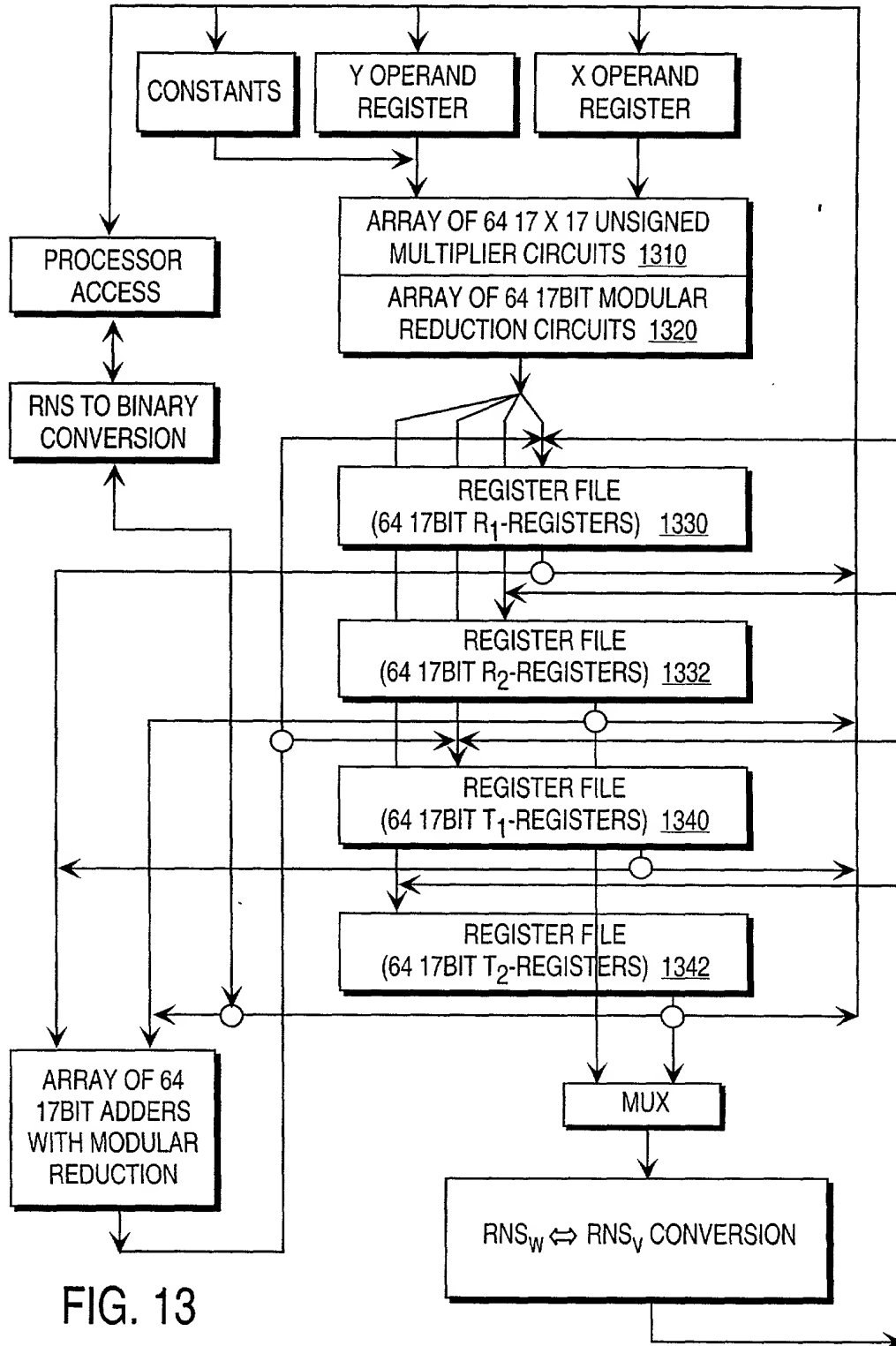
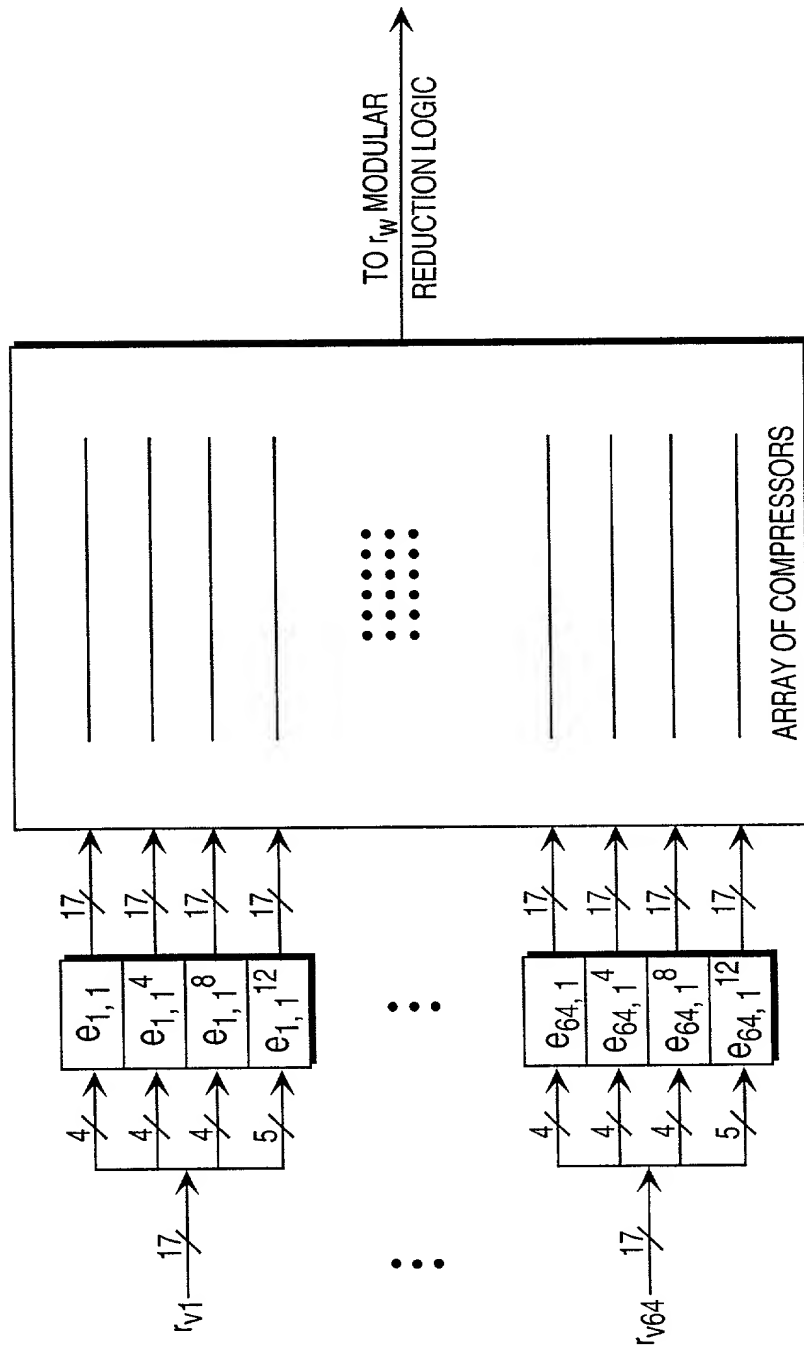


FIG. 13



SINGLE RAW COMPUTATION (SRC) MODULE

FIG. 14

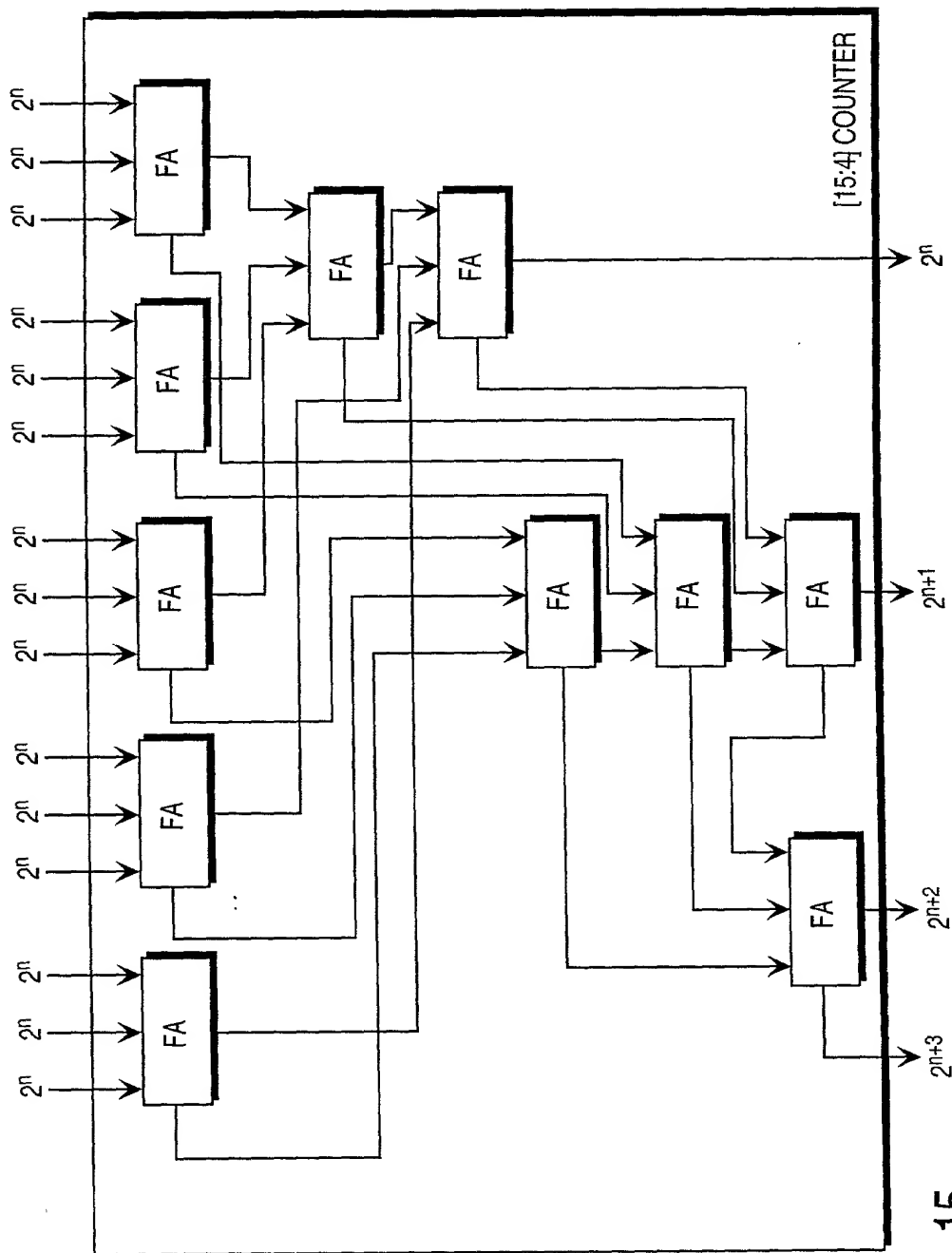


FIG. 15

19 / 28

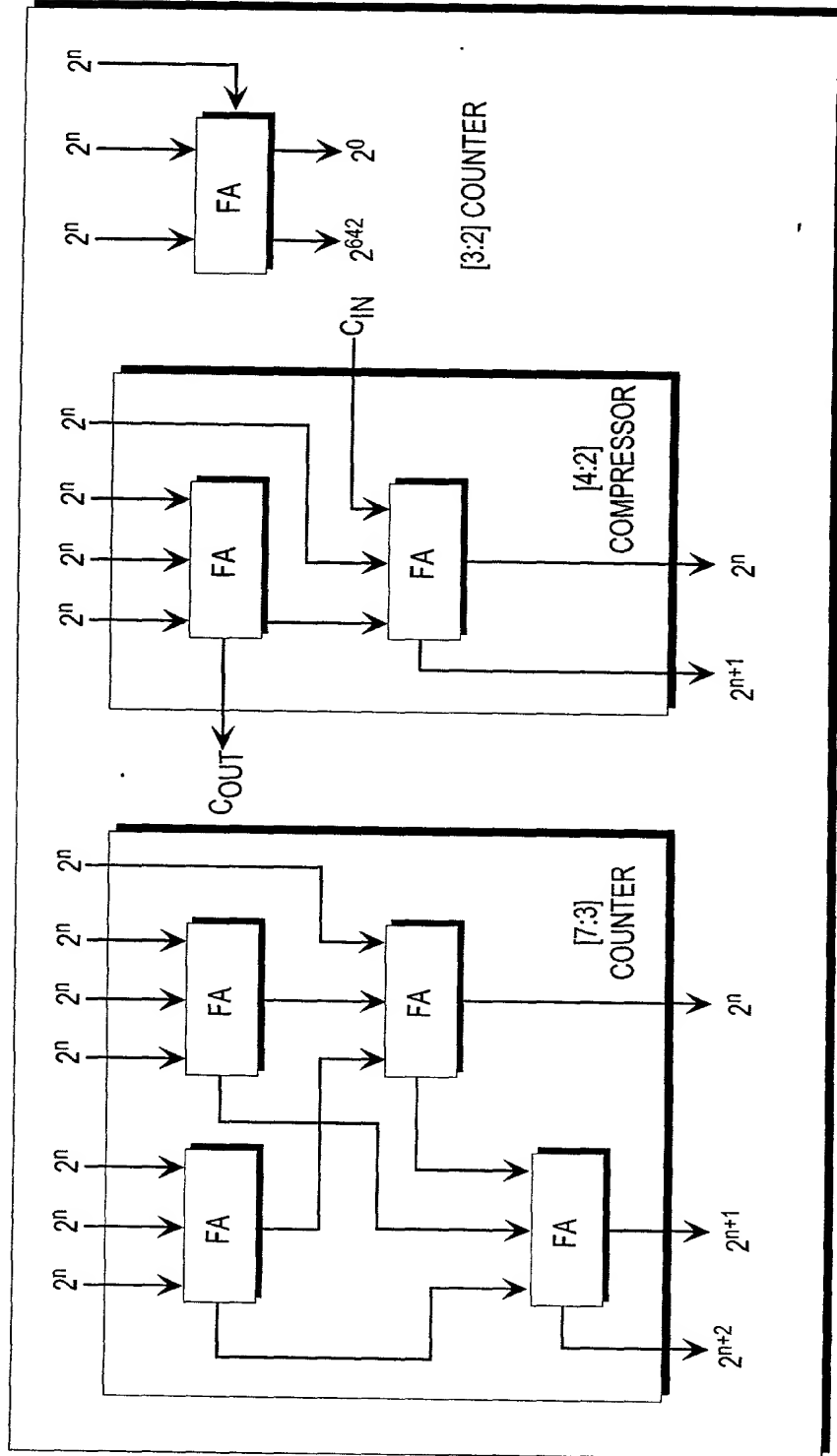


FIG. 16

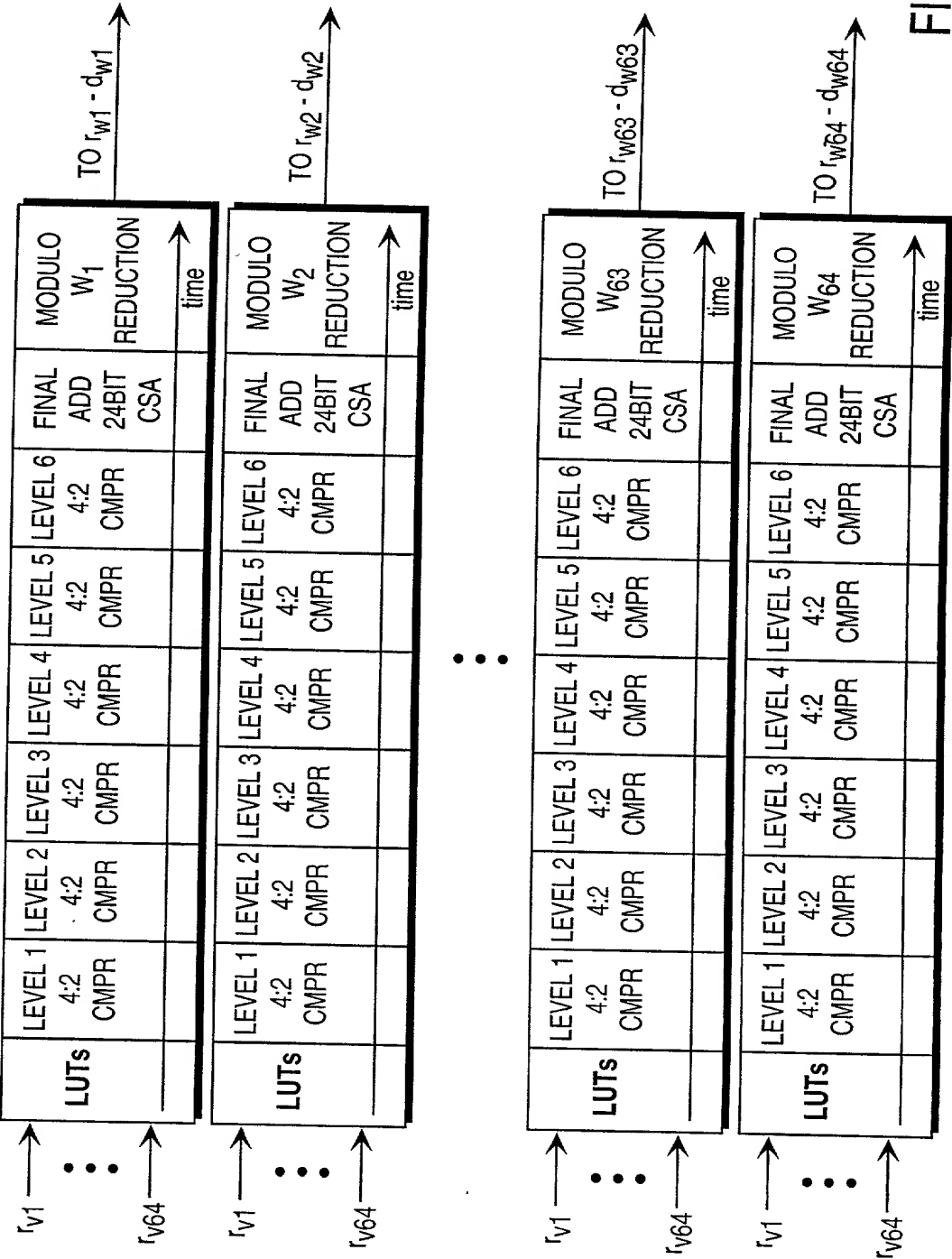


FIG. 17

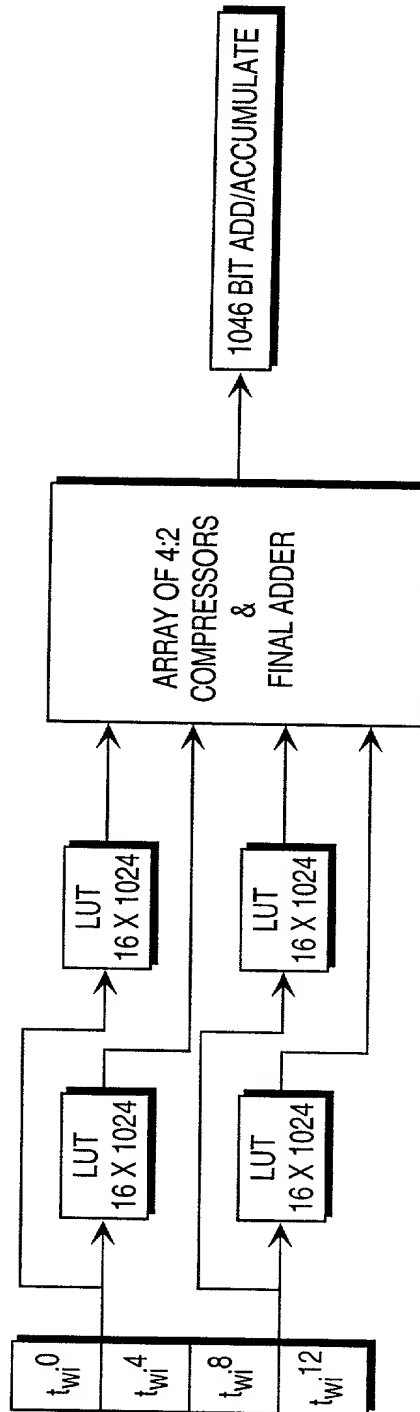


FIG. 18

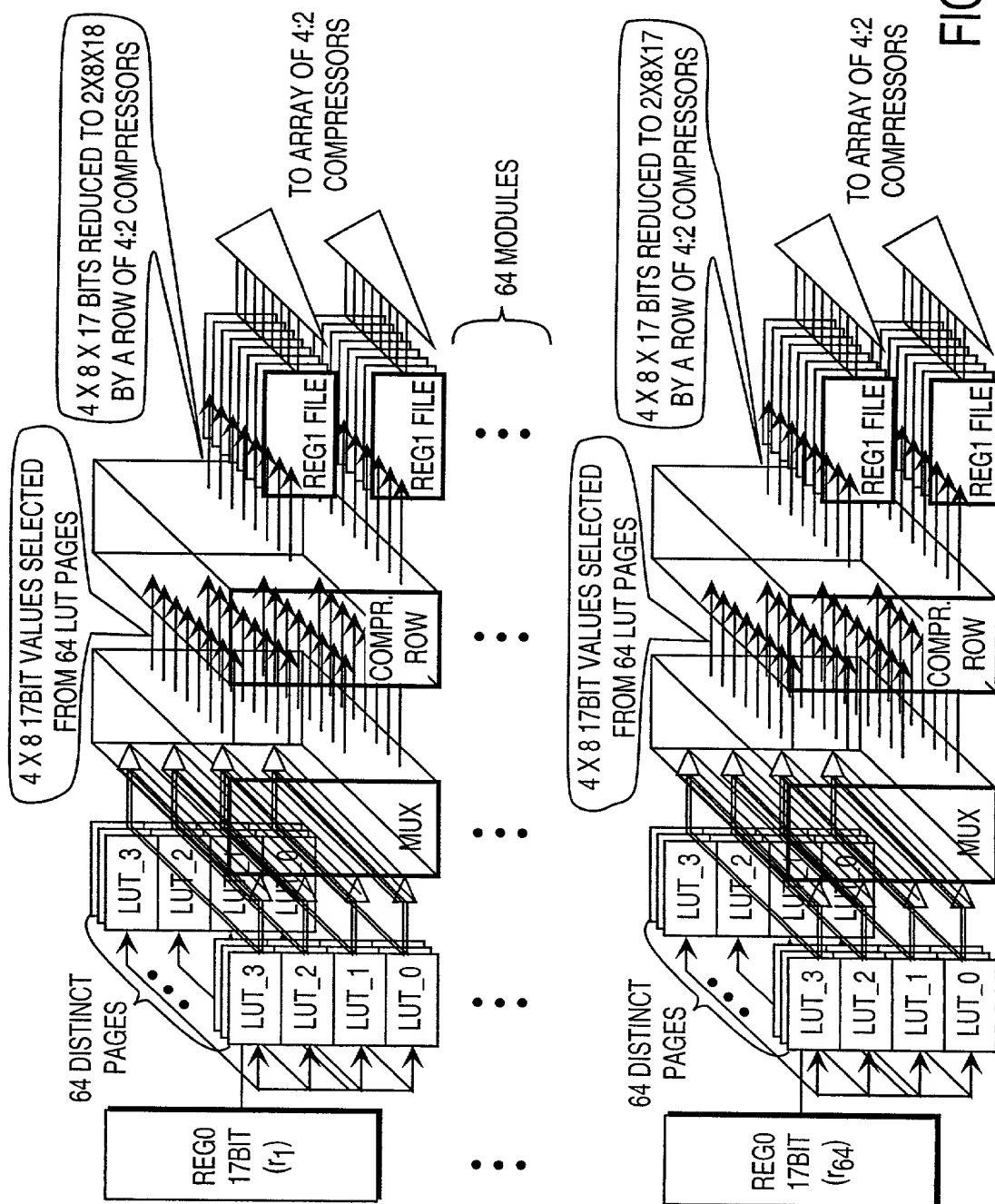


FIG. 19

23 / 28

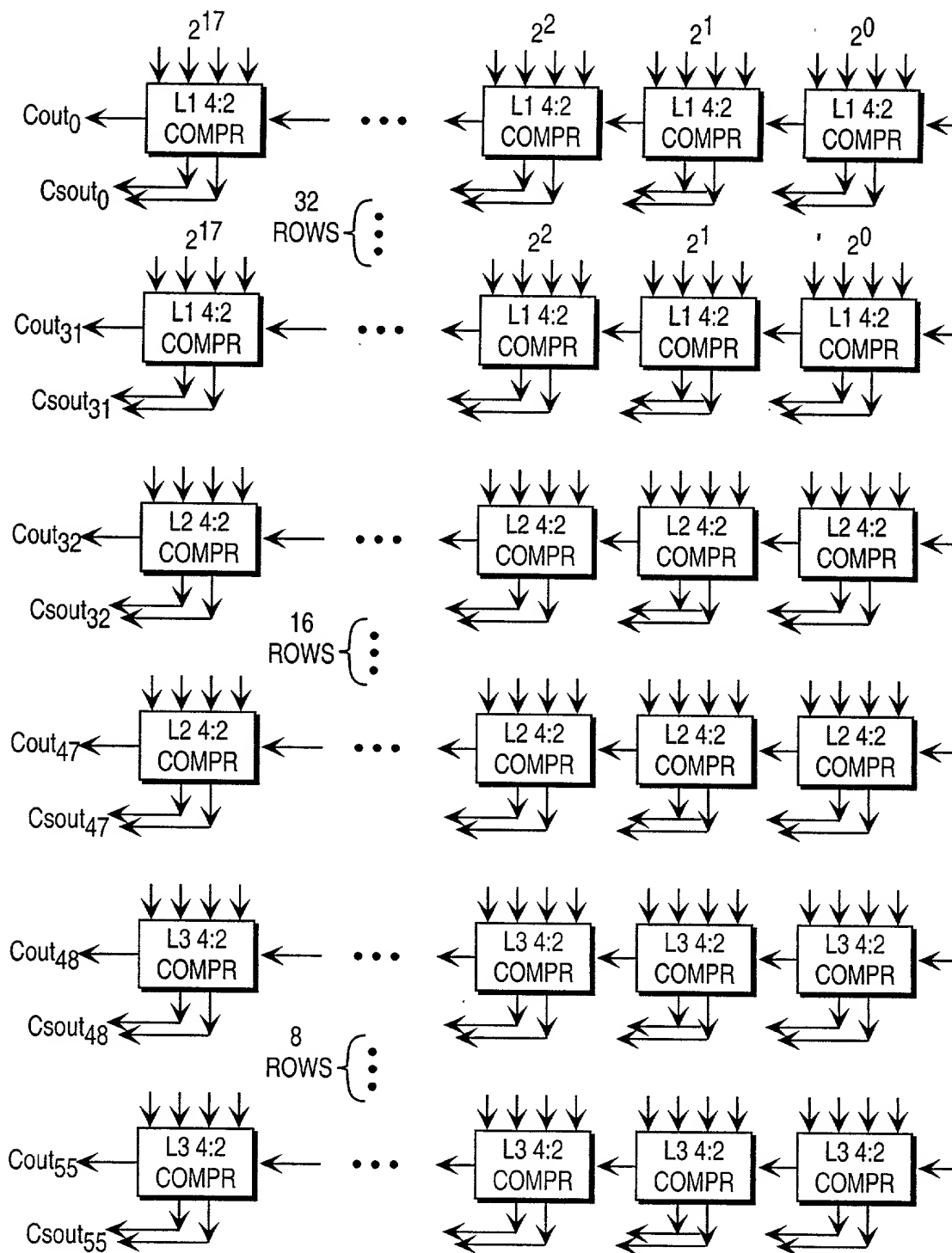


FIG. 20A

CONTINUED ON FIG. 20B

24 / 28

CONTINUED FROM FIG. 20A

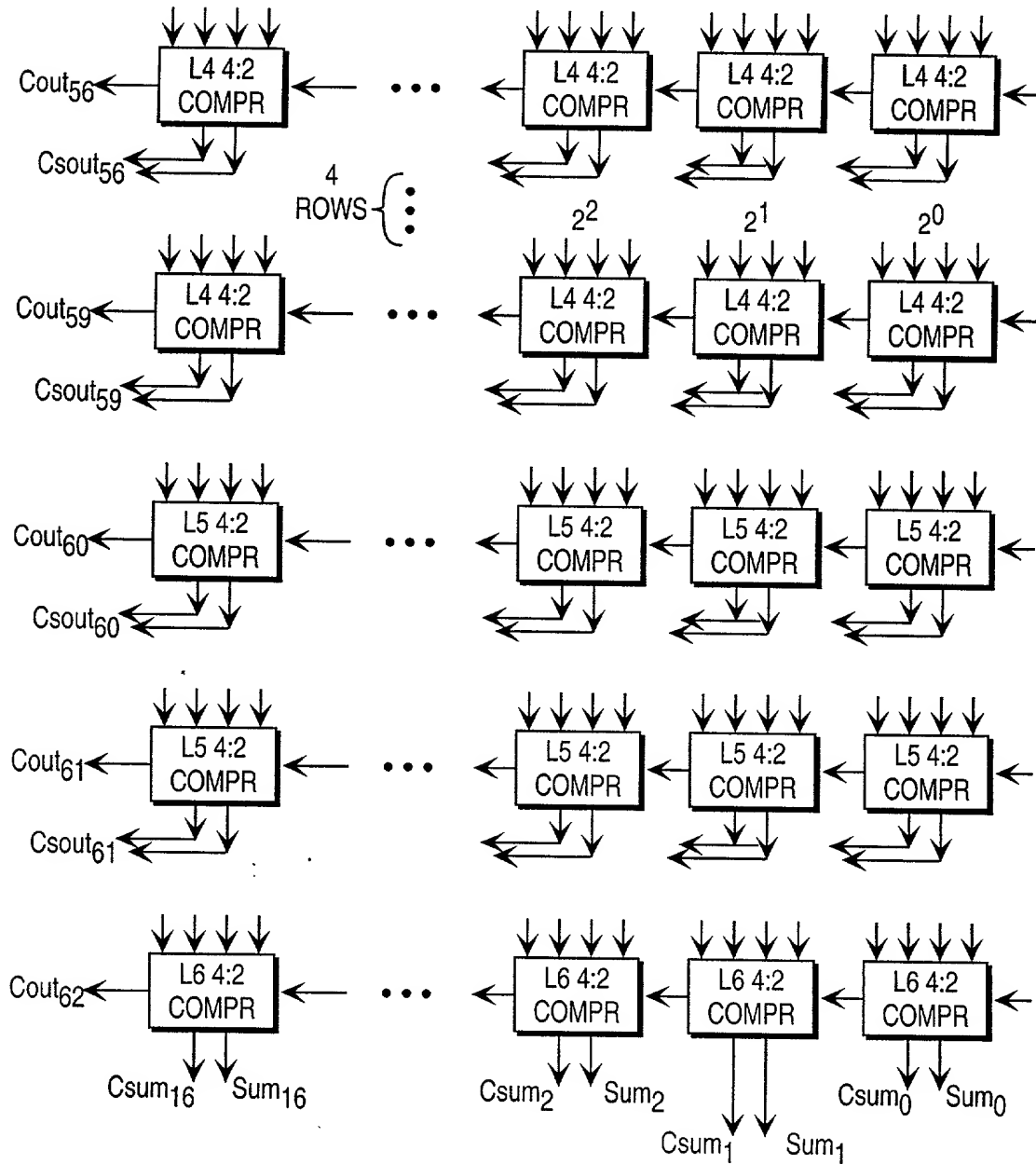


FIG. 20B

8 PLANES OF PIPELINED HARDWARE
 FOR SIMULTANEOUS EXECUTION

FIG. 21

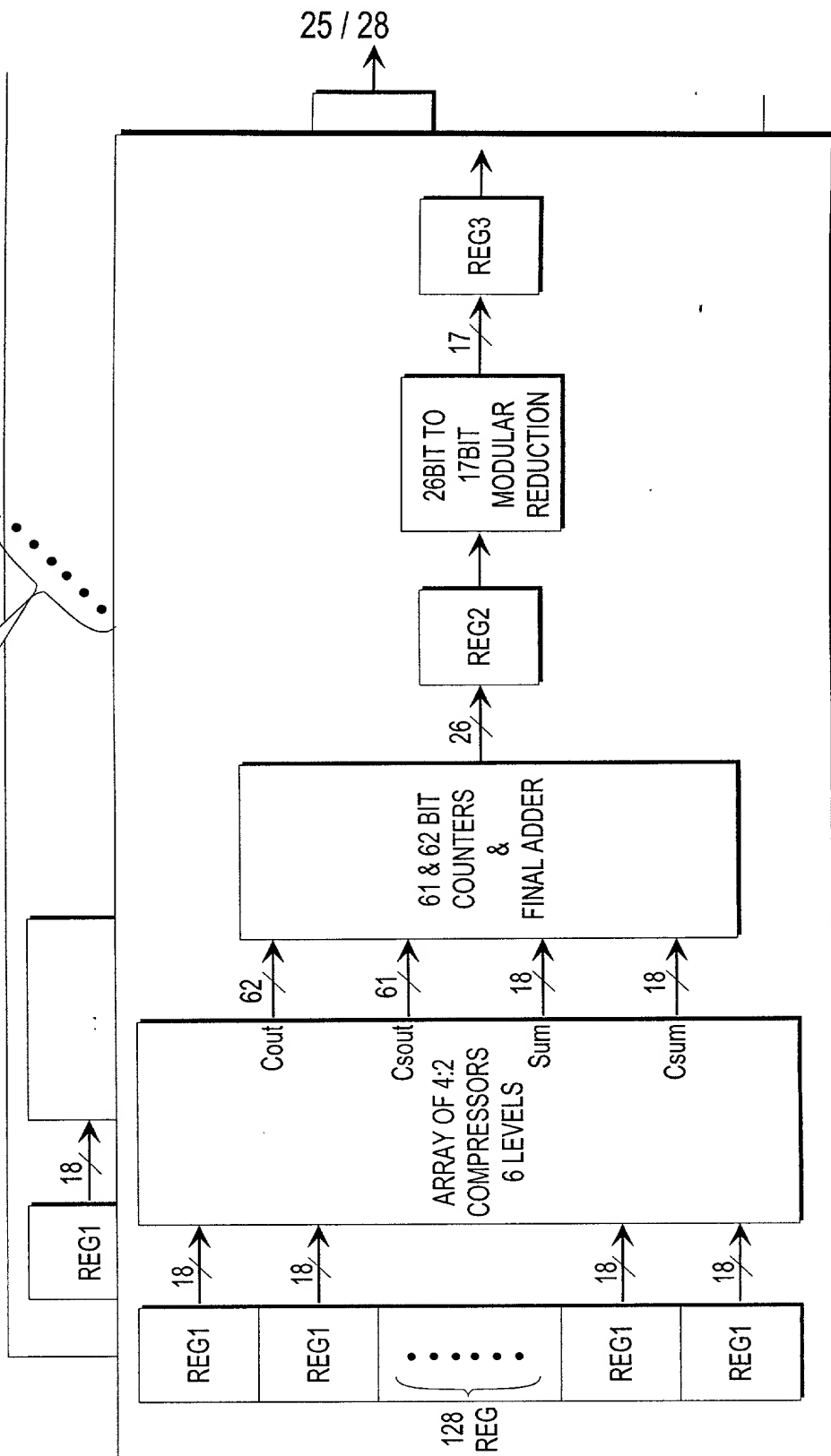
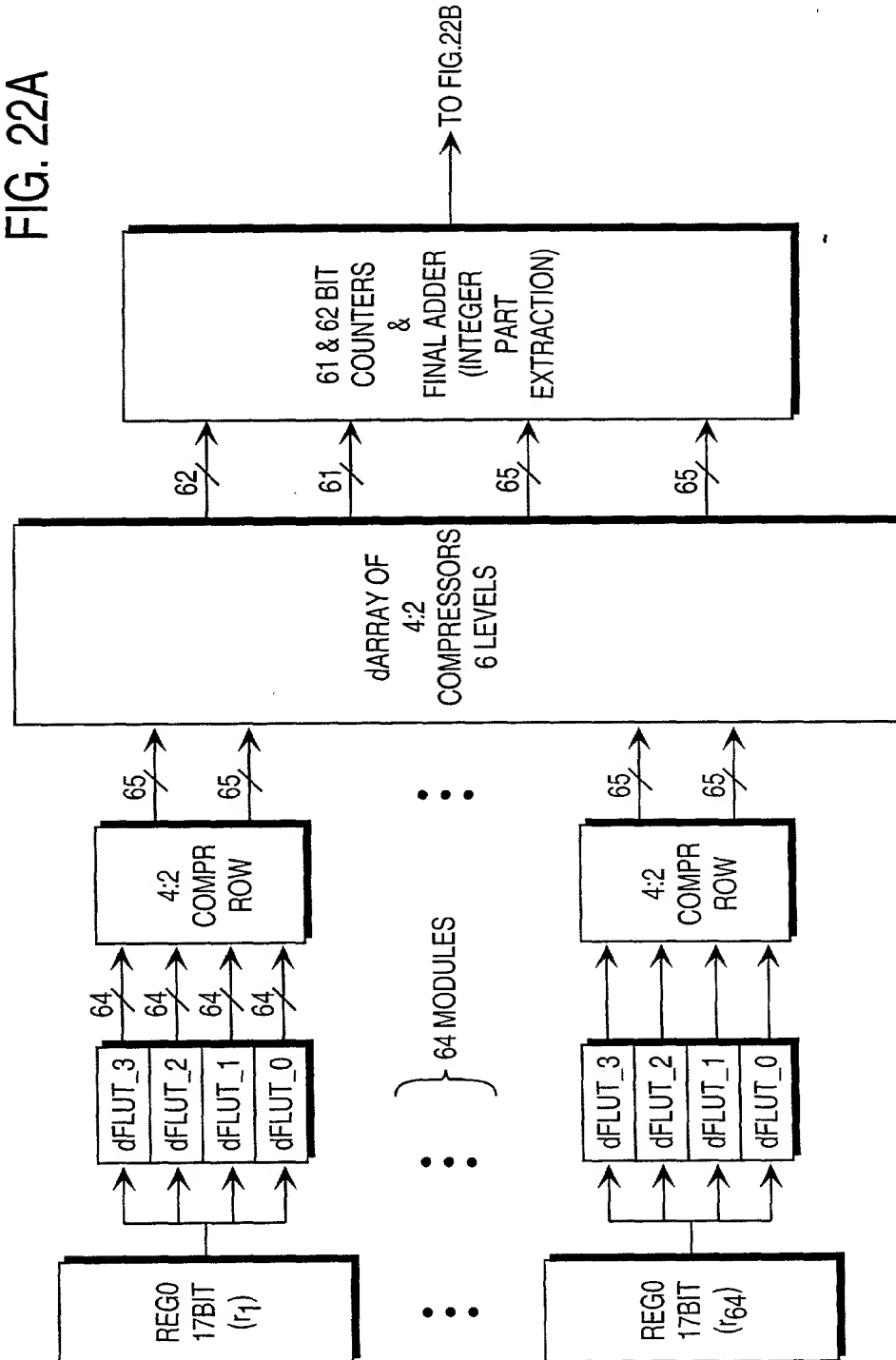


FIG. 22A



27 / 28

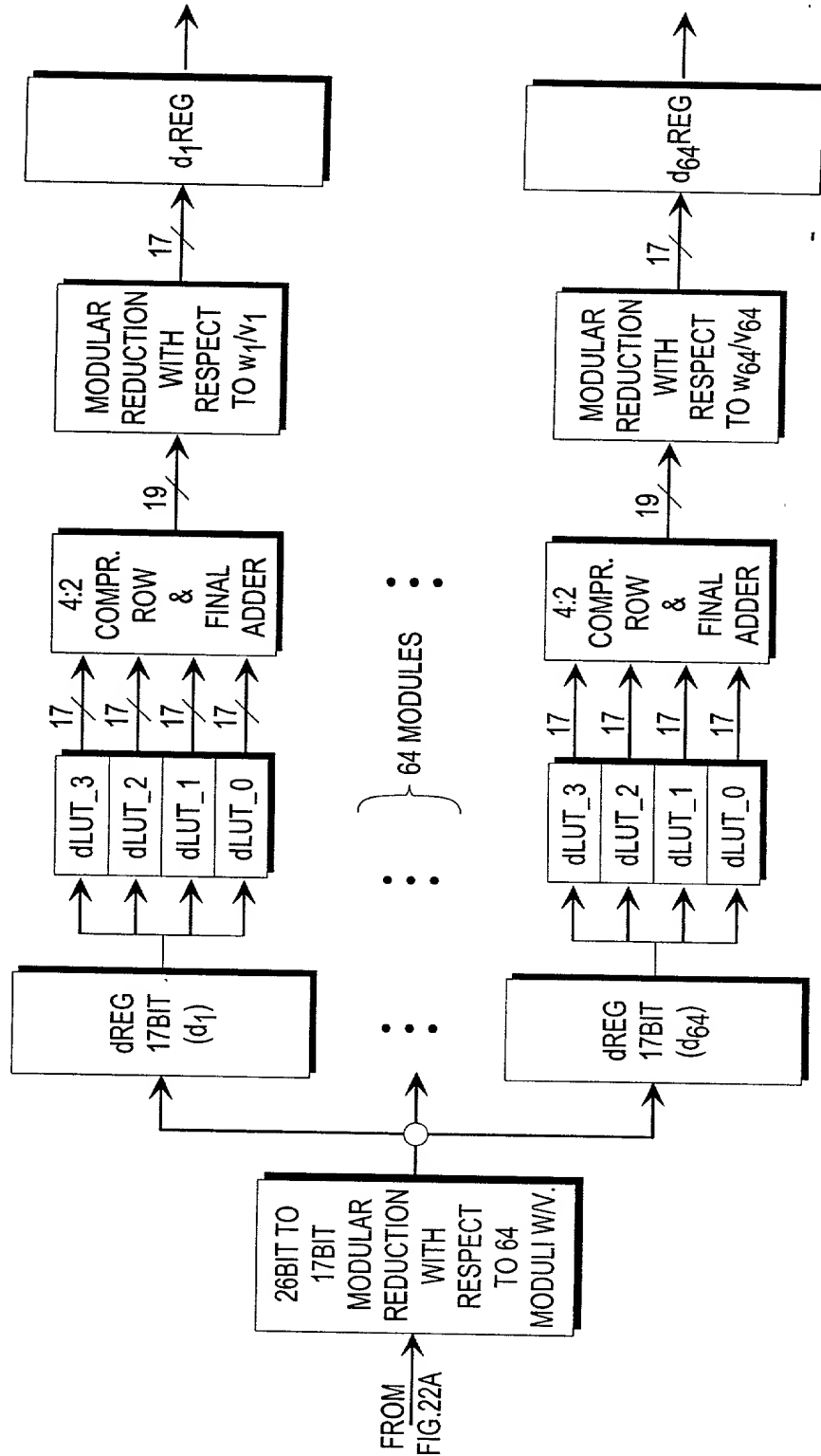


FIG. 22B

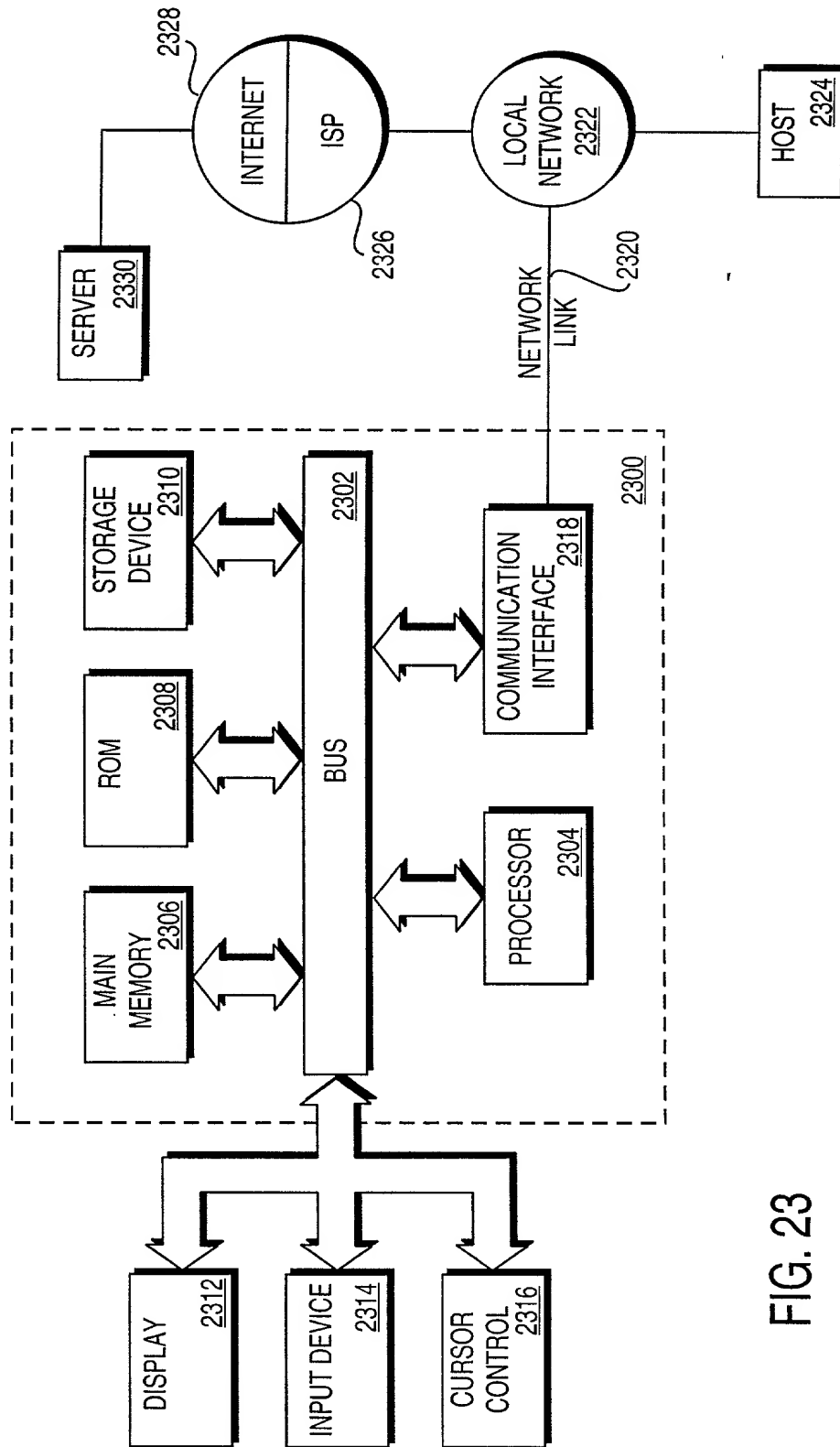


FIG. 23